Geheime Kommandosache.

Chi. IV c Berlin, 25. August 1944

Aktenvermerk

Betrifft: Sicherheit der Enigma.

Der Sonderausschuß zur Überprüfung der Sicherheit eigener Geheimschriften behandelte am 4. und 15.August 1944 die verschiedenen Typen der Enigma.

Auf der 1.Arbeitstagung wurden die verschiedenen Lösungsmöglichkeiten durchgesprochen. Ergebnis:

1. Die K-Maschinen bieten keinerlei Sicherheit. Der einzelne Geheimtext kann mit verhältnismässig einfachen maschinellen Hilfsmitteln in durchaus tragbarer Zeit entziffert werden.

2. Die G-Maschinen genügen nicht zeitgemässen Sicherheitsansprüchen. Der einzelne Geheimtext kann mit einem grösseren Aufwand an maschinellen Hilfsmitteln in tragbarer Zeit entziffert werden.

3. Für die Heeres-Enigma (Steckerbrett, 3 Walzen mit je 1 Lücke) werden theoretische Lösungen gesehen, deren praktische Durchführung bei erheblichem maschinellen Aufwand im Bereich des Möglichen liegt. Bei der Marine-Enigma (Steckerbrett, 4 Walzen mit je 2 Lücken) erscheint der Aufwand an Hilfsgeräten und Zeit zu gross, als dass Geheimtexte in tragbarer Zeit entziffert werden könnten.

Auf der 2.Arbeitstagung wurden die verschiedenen Schlüsselvorschriften durchgesprochen. Ergebnis:

1. K-Maschine.

Eine mechanische Veränderung an den K-Maschinen zur Erhöhung der Sicherheit erscheint nicht durchführbar. K-Maschinen dürfen zur Übermittlung geheimer Nachrichten nur dann noch verwendet werden, wenn der Klartext mit der Maschine zweimal verschlüsselt wird. Es erscheint dabei tragbar, dass die eine Verschlüsselung mit einer festen Grundstellung erfolgt, wenn die andere Verschlüsselung nach der Spruchschlüsseltechnik der Heeres-Enigma, bzw. nach einer hiermit gleichwertigen Schlüsseltechnik erfolgt.

2.

2. G-Maschine.

Eine mechanische Veränderung an den G-Maschinen zur Erhöhung der Sicherheit erscheint nicht durchführbar. G-Maschinen dürfen zur Übermittlung geheimer Nachrichten nur dann verwendet werden, wenn der Klartext zuvor mit einem Versatzverfahren verschlüsselt wird. Es erscheint dabei tragbar, dass das Versatzverfahren ein einfacher Würfel konstanter Breite und aufsteigender Losung ist. Als Mindestbreite muss 10 und als Mindesttiefe 5 gefordert werden. Kurze Klartexte müssen auf mindestens 50 Buchstaben aufgefüllt werden. Die Maschinen-Verschlüsselung hat nach der Spruchschlüsseltechnik der Heeres-Enigma bzw. nach einer hiermit gleichwertigen Schlüsseltechnik zu erfolgen.

3. Stecker-Maschine.

Zur Erhöhung der Sicherheit der Stecker-Enigma sind folgende Vorschriften, Neuerungen bzw. Zusatzgeräte vorgesehen:

a) Verstellen der linken Walze nach je 70 - 130 Buchstaben.
b) Lückenfüllerwalzen.
c) Enigma-Stecker-Uhr.

Zu a) Im Heer ist das Verstellen der linken Walze im festen Funknetz bereits eingeführt; im Feldheer soll die Verstellung in Kürze eingeführt werden. Die maximale Spruchlänge kann dann auf 500 Buchstaben heraufgesetzt werden. In der Luftwaffe wird das Verstellen nicht durchgeführt, da dort überall D-Walzen vorhanden sind. Maximale Spruchlänge bleibt 250 Buchstaben.

Zu b) Die Vorschrift zur Anwendung der Lückenfüllerwalzen wird vom Heer ausgearbeitet.

Zu c) Luftwaffe hat den 2.Vorschlag der Ag N eingeführt. Heer wird ihn einführen.

Die einzelnen Vorschriften zur Anwendung der Stecker-Maschinen wurden durchgesprochen und folgendermassen beurteilt:

A) Heer.

Die Spruchschlüsselableitung genügt so lange den Sicherheitsanforderungen, wie ein Einbruch nicht erfolgt ist. Ist ein Einbruch erfolgt, so kann laufend mitgelesen werden.

Der

Der augenblicklich angewendete Notschlüssel genügt nicht mehr, da er nur für einen Tag gilt. Neuentwicklung wird vorgeschlagen.

B) Luft.

Die Luftwaffe schlüsselt nach denselben Vorschriften wie das Heer.

C) Marine.

Schlüssel- und Verfahrens-Kenngruppen werden mit 9 in grösseren Zeitabständen wechselnden Paartauschtafeln überschlüsselt. Schwäche ist die gleichbleibende Grundstellung. Änderung ist in Arbeit.

Der Notschlüssel genügt nicht zeitgemässen Sicherheitsansprüchen und muss durch einen geeigneten Notschlüssel ersetzt werden. Dabei sollen die planmässigen Unterlagen benutzt werden können. Änderung ist in Arbeit.

D) Agentenverkehr.

Die Vorschrift Nr.63 genügt nur dann zeitgemässen Sicherheitsansprüchen, wenn auf jeder Linie nur wenig Verkehr auftritt. Es soll versucht werden, eine bessere Vorschrift auszuarbeiten.

Es wird dafür gesorgt werden, dass alle anderen mit Enigma-Maschinen arbeitenden Behörden usw. nur die vom Ausschuss geprüften und zugelassenen Vorschriften benutzen.

E) Sonderschlüssel.

1) Stabsmaschinenschlüssel. Es wird zeitliche Unterteilung vorgeschlagen.
2) Chefsachen. Es werden gesonderte Schlüsselunterlagen vorgeschlagen. Es wird geprüft, ob vom betrieblichen Standpunkt doppelte Verschlüsselung tragbar ist.

Geheime Kommandosache.

C h i IV c Berlin, 5. Sept. 1944

A k t e n v e r m e r k

Betrifft: Sicherheit der SFM T 52

Der Sonderausschuß zur Überprüfung der Sicherheit eigener Geheimschriften behandelte am 25. August 1944 die verschiedenen Typen der Schlüsselfernschreibmaschine T 52. Als Ergebnis wurde festgestellt

1. Die SFM T 52 c genügt nicht zeitgemäßen Sicherheitsforderungen. Ein einzelner Geheimtext kann mit maschinellen Hilfsmitteln in tragbarer Zeit entziffert werden.

2. Die SFM T 52 d wird für die Verschlüsselung von Geheimen Kommandosachen und für den Einsatz auf Funkfernschreiblinien als ausreichend sicher angesehen. Die Vorschrift zur Verwendung von Wahlwörtern muß beibehalten werden, die Beschränkung der Spruchlängen auf 20 000 Zeichen kann jedoch fortfallen. Da die jetzige (feste) KT-Funktion Einbruchsmöglichkeiten über Kompromisse begünstigt, wird sie nicht eingesetzt. Für den Grundschlüssel dürfen nur nicht zerfallende Pyramiden benutzt werden.

3. Für die SFM T 52 e liegen noch keine eingehenden Sicherheitsuntersuchungen vor. Einsatz auf Funkfernschreiblinien und Verschlüsselung von Geheimen Kommandosachen mit T 52 e ist zulässig. Wie bei der T 52 d müssen Wahlwörter verwendet werden. Beschränkung der Spruchlängen und Verwendung der KT-Funktion sind nicht erforderlich.

Geheime Kommandosache

C h i. IV c Berlin, 26. Sept. 1944

Betrifft: Sicherheit der SZ 40 und 42

A k t e n v e r m e r k

Der Sonderausschuß zur Überprüfung der Sicherheit eigener Geheimschriften behandelte am 11.9. die Schlüsselzusätze 40 und 42. Als Ergebnis wurde festgestellt:

Ein zusammenhängender Geheimtext von 30 000 - 40 000 Buchstaben ist lösbar. Phasengleiche Sprüche können gelöst werden, ebenso Sammelsprüche von 1 000 Buchstaben an. Aus einem Kompromiß (Zuordnung von Klar- und Geheimtext) von etwa 500 Buchstaben ist die Nockenbestückung rekonstruierbar.

Die Schlüsselzusätze 40 und 42 dürfen daher nur im Linienverkehr eingesetzt werden, weil hier phasengleiche Sprüche, Sammelsprüche und Kompromisse vermieden werden können. Doch ist notwendig, daß

a) jede Linie mit besonderen Schlüsseln ausgestattet wird,
b) die Schlüssel täglich wechseln,
c) die Spruchlänge auf 10 000 Buchstaben beschränkt wird.

Soweit betrieblich möglich, soll mit KT-Funktion gearbeitet werden.

Die Sicherheitsuntersuchungen des SZ 42 c sind noch nicht abgeschlossen. Bis jetzt wird keine Möglichkeit gesehen, aus reinem Schlüsseltext die Maschineneinstellung zu rekonstruieren.

Geheime Kommandosache.

C h i IV c Berlin, 10. Oktober 1944

Betrifft: Sicherheit der Rufzeichenverschlüsselung und der Handschlüsselverfahren NS 42, TS 42a und Raster RS 44

A k t e n v e r m e r k

Der Sonderausschuß zur Überprüfung der Sicherheit eigener Geheimschriften behandelte am 26.9. die Rufzeichenverschlüsselung und Handschlüsselverfahren NS 42, TS 42a und RS 44. Als Ergebnis wurde festgestellt:

1. Rufzeichenverschlüsselung:

Die bisher in Heer und Luftwaffe angewendeten Systeme der Rufzeichenverteilung genügen nicht zeitgemäßen Sicherheitsforderungen. Ist die Grundrufzeichenverteilung bekannt, so genügt zur Lösung die Identifizierung eines Rufzeichens. Ist die Grundrufzeichenverteilung nicht bekannt, so ist zur Lösung das Material von 4-5 Tagen notwendig.

Gegen die zur Einführung vorgesehene Rufzeichenverschlüsselung, sowie gegen die freie Wahl der Rufzeichen bestehen keine Bedenken.

Ein Wechsel der Geheimrufzeichen ist nur dann voll wirksam, wenn zugleich die Frequenzen gewechselt werden.

2. NS 42:

Die Lösung gelingt für ein Kastenpaar ohne besonderen Aufwand mit 3 000 Buchstaben Geheimtext, in günstigen Fällen schon mit 1 000 Buchstaben.

3. TS 42a:

Die Lösung gelingt mit ca. 600 Buchstaben Geheimtext.

Die Sicherheit des NS 42 und TS 42a wird für nicht ausreichend angesehen.

4. RS 44:

Eine Lösungsmöglichkeit für den einzelnen Spruch wird nicht gesehen.

Schlüssel- und längengleiche bzw. schlüssel- und längenähnliche Sprüche können zur Lösung führen. Da solche Sprüche nur in Ausnahmefällen an den Spruchschlüsseln erkennbar sind, ist ein Einbruch auf diesem Wege unwahrscheinlich

und

und auch dann nur unter großem Aufwand möglich. Ist einmal ein Einbruch erfolgt, so kann mit großem Aufwand die Lösung weiterer Sprüche und die vollständige Rekonstruktion aller Unterlagen erfolgen.

Da bei vorschriftsmäßiger Anwendung die Wahrscheinlichkeit für diese Einbruchsmöglichkeiten gering und der Aufwand in jedem Falle sehr groß ist, wird die Sicherheit des Rasterverfahrens für ausreichend gehalten.

Gegen die freie Wahl der Anfangsspalte des Herauslesens bestehen keine Bedenken.

Für die Truppennachrichtenverbände kann die Mindestspruchlänge auf 45 Buchstaben herabgesetzt werden.